

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

1                   1 (currently amended): A method of authenticating a client to a server  
2 comprising:  
3                   generating a challenge at the client;  
4                   signing the challenge to form a signed challenge;  
5                   sending at least the signed challenge to the server, where the authenticity of the  
6 server is not in questions question;  
7                   verifying the signature of the challenge at the server; and  
8                   if the signature is verified, sending an indication of successful authentication to  
9 the client, where the indication of successful authentication is generated employing a single  
10 round trip authentication scheme.

1                   2 (original): The method of claim 1, wherein generating a challenge at the client  
2 comprises generating a random number.

1                   3 (original): The method of claim 1, wherein generating a challenge at the client  
2 comprises generating a sequential challenge.

1                   4 (original): The method of claim 1, wherein generating a challenge at the client  
2 comprises generating a challenge based on data received from the server in a prior step.

1                   5 (original): The method of claim 4, wherein the data received from the server is  
2 a challenge returned with a server response to a prior client query.

1                   6 (previously presented): A method of using a one-time use card number for an  
2 online transaction, comprising:

3                   generating a one-time use card number at a user system using a random number  
4 generator;  
5                   authenticating the user system to an issuer system, where the authenticating  
6 employs a single round trip authentication scheme;  
7                   passing the one-time use card number from the user system to the issuer system;  
8                   passing the one-time use card number from the user system to a merchant system,  
9 wherein the merchant system is programmed to present the one-time use card number to the  
10 issuer system to effect a payment;  
11                  verifying the one-time use card number received from the merchant system with  
12 the one-time use card number received from the user system; and  
13                  if the one-time use card number is verified, approving the transaction.

1                  7 (original): The method of claim 6, wherein passing the one-time use card  
2 number to the issuer includes passing at least one other data element related to the online  
3 transaction.

1                  8 (original): The method of claim 7, wherein the at least one other data element  
2 is selected from, or a function of, a user's account number, a user's private key, a transaction  
3 time, a transaction amount, or a merchant ID.